

CLAIMS

What is claimed is:

1. A method for producing a secure key, the method comprising:
receiving at least a first input key, a second input key and a third input key; and
generating a first output key based on said at least said first input key, said second input key and said third input key, wherein said first output key is unique and differs from said at least said first input key.

2. The method according to claim 1, wherein said first input key is a customer key, said second input key is a customer key selection and said third input key is a key variation.

3. The method according to claim 1, further comprising:
determining whether said first output key is at least one of a unique key and is not equivalent to said at least said first input key; and
if said first output key is at least one of a non-unique key and is equivalent to said at least said first input key, generating a second output key based on a modified one of at least one of said first input key, said second input key and said third input key.

4. The method according to claim 3, further comprising determining whether said second output key is at least one of a unique key and is not equivalent to said at

least said modified one of at least one of said first input key, said second input key and said third input key.

5. The method according to claim 4, wherein said first output key and said second output key are not weak or semi-weak keys.

6. The method according to claim 1, further comprising mapping said at least said first input key, said second input key and said third input key to generate mapped output key data.

7. The method according to claim 6, further comprising generating an intermediate key based on said first input key.

8. The method according to claim 7, further comprising scrambling said generated intermediate key and said generated mapped output key data to create a scrambled output.

9. The method according to claim 8, further comprising:
masking at least a portion of said generated mapped output key data; and
exclusive ORing said masked at least said portion of said generated mapped output key data and said scrambled output to generate said first output key.

10. The method according to claim 1, further comprising transferring said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information.

11. A machine-readable storage having stored thereon, a computer program having at least one code section for producing a secure key, the at least one code section being executable by a machine for causing the machine to perform steps comprising:

receiving at least a first input key, a second input key and a third input key; and generating a first output key based on said at least said first input key, said second input key and said third input key, wherein said first output key is unique and differs from said at least said first input key.

12. The machine-readable storage according to claim 11, wherein said first input key is a customer key, said second input key is a customer key selection and said third input key is a key variation.

13. The machine-readable storage according to claim 11, further comprising:
code for determining whether said first output key is at least one of a unique key and is not equivalent to said at least said first input key; and
code for generating a second output key based on a modified one of at least one of said first input key, said second input key and said third input key if said first output

key is at least one of a non-unique key and is equivalent to said at least said first input key.

14. The machine-readable storage according to claim 13, further comprising code for determining whether said second output key is at least one of a unique key and is not equivalent to said at least said modified one of at least one of said first input key, said second input key and said third input key.

15. The machine-readable storage according to claim 14, wherein said first output key and said second output key are not weak or semi-weak keys.

16. The machine-readable storage according to claim 11, further comprising code for mapping said at least said first input key, said second input key and said third input key to generate mapped output key data.

17. The machine-readable storage according to claim 16, further comprising code for generating an intermediate key based on said first input key.

18. The machine-readable storage according to claim 17, further comprising code for scrambling said generated intermediate key and said generated mapped output key data to create a scrambled output.

19. The machine-readable storage according to claim 18, further comprising:
code for masking at least a portion of said generated mapped output key data;
and

code for exclusive ORing said masked at least said portion of said generated
mapped output key data and said scrambled output to generate said first output key .

20. The machine-readable storage according to claim 11, further comprising
code for transferring said generated first output key to an encryption engine that utilizes
said generated first output key to encrypt information.

21. A system for producing a secure key, the system comprising:
a secure key generator that receives at least a first input key, a second input key
and a third input key; and

said secure key generator generates a first output key based on said at least said
first input key, said second input key and said third input key, wherein said first output
key is unique and differs from said at least said first input key.

22. The system according to claim 21, wherein said first input key is a
customer key, said second input key is a customer key selection and said third input key
is a key variation.

23. The system according to claim 21, wherein said secure key generator:

determines whether said first output key is at least one of a unique key and is not equivalent to said at least said first input key; and

generates a second output key based on a modified one of at least one of said first input key, said second input key and said third input key, if said first output key is at least one of a non-unique key and is equivalent to said at least said first input key.

24. The system according to claim 23, wherein said secure key generator determines whether said second output key is at least one of a unique key and is not equivalent to said at least said modified one of at least one of said first input key, said second input key and said third input key.

25. The system according to claim 24, wherein said first output key and said second output key are not weak or semi-weak keys.

26. The system according to claim 21, further comprising a mapper that maps said at least said first input key, said second input key and said third input key to generate mapped output key data.

27. The system according to claim 26, further comprising a key generator that generates an intermediate key based on said first input key.

28. The system according to claim 27, further comprising a scrambler that scrambles said generated intermediate key and said generated mapped output key data to create a scrambled output.

29. The system according to claim 28, further comprising:
a masker that masks at least a portion of said generated mapped output key data; and
an exclusive OR operator that exclusive ORs said masked at least said portion of said generated mapped output key data and said scrambled output to generate said first output key.

30. The system according to claim 21, wherein said secure key generator transfers said generated first output key to an encryption engine that utilizes said generated first output key to encrypt information.

31. A system for producing a secure key, the system comprising:
a mapper;
a scrambler coupled to said mapper;
a masker coupled to said mapper;
a key generator coupled to said scrambler; and
an XOR operator coupled to said masker and said scrambler.

32. The system according to claim 31, further comprising at least one processor coupled to an output of said XOR operator.

33. The system according to claim 32, further comprising an encryption engine that is coupled to an output of said XOR operator.

34. The system according to claim 33, further comprising a memory coupled to at least one of said encryption engine and said at least one processor.